AMENDMENTS TO THE DRAWINGS

The attached "Replacement Sheet" of drawings includes changes to Figure 1. The attached "Replacement Sheet," which includes Figure 1, replaces the original sheet including Figure 1.

Attachment: Replacement Sheet

REMARKS

Claims 19-40 are now pending in the application. Claims 1-18 have been cancelled. Claims 19-40 have been added as new. Various amendments have been made to the specification, abstract, and drawings. No new matter has been added, as support for the amendments may be found throughout the specification, claims, and drawings as originally filed. The Examiner is respectfully requested to consider the amendments and remarks contained herein.

DRAWINGS

Applicant has attached a revised drawing for the Examiner's approval. In the "Replacement Sheet" Applicant has added the legend --Prior Art-- to Figure 1.

REJECTION UNDER 35 U.S.C. § 112

Claims 1 and 8 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point and distinctly claim the subject matter which Applicant regards as the invention. This rejection is respectfully traversed.

Applicant has cancelled claims 1 and 8 hereby rendering this rejection moot.

REJECTION UNDER 35 U.S.C. § 103

Claims 1-7 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Frankel et al. (U.S. Pat. No. 6,035,041) in view of Brickell et al. (U.S. Pat. No.

6,959,394) and Brennan et al. (U.S. Pat. No. 5,675,649). This rejection is respectfully traversed.

Applicant has cancelled claims 1-7 hereby rendering this rejection moot.

Applicant respectfully submits that the independent claims 19 and 37 define over the art cited by the Examiner.

Frankel at best discloses a cryptographic system. In the cryptographic system the input processor provides all of the agents with information relating to the particular cryptographic service request, and the agent applies its individual key shares to generate partial result through a calculation, and the agent sends the partial result to an output processor. The output processor takes the partial result from the agent, and uses an equation to combine the partial result to get a result of the cryptographic system (see column 4 lines 20-58 of Frankel). Frankel fails to teach or suggest the following elements recited in Claim 19:

Element 1: "the offline secret key distributor is configured for splitting a private key into multiple first sub-secret-keys d_{ji} and multiple second sub-secret-keys, sending the first sub-secret-keys d_{ji} to the k online secret share calculators; sending the second sub-secret-keys and equation combination representations corresponding to the second sub-secret-keys to the m online secret share combiners; and the private key is constructed by one second sub-secret-key and t first sub-secret-keys d_{ji}, each equation combination representation comprises t items of j and i, j is sequence number of the secret share calculator and i is number of the first sub-secret-key in the j^{th} secret share calculator, and each of j in one equation combination representation is different."

Element 2: "the k online secret share calculators are configured for checking correctness of the certificate to be signed, calculating at least t first calculation results according to first sub-secret-keys stored and the certificate to be signed, and sending out the at least t first calculation results, at least t items of j and i corresponding to the at least t first calculation results respectively through a second broadcast channel."

Element 3: "the m online secret share combiners are configured for matching t items of j and i received through the second broadcast channel with the equation combination representations stored, and determining a matched online secret combiner storing the matched equation combination representation including t items of j and i;

the matched online secret share combiner is configured for checking the correctness of the certificate to be signed, calculating a second calculation result according to the certificate to be signed and the second sub-secret-key corresponding to the matched equation combination representation, calculating a digital signature according to the t first calculation results corresponding to the t items of i and j in the matched equation combination representation and the second calculation result, generating a digital certificate according to the digital signature and contents of the certificate to be signed."

Claim 37 discloses a method corresponding to the system of claim 19. Frankel likewise fails to teach or suggest the following features defined in the amended claim 37:

Element 1: "splitting a private key into multiple first sub-secret-keys and multiple second sub-secret-keys, wherein the private key is constructed by one second sub-

secret-key and t first sub-secret-keys, the second sub-secret-key corresponds to the t first sub-secret-keys according to an equation combination representation, and the number t is a positive integer."

Element 2: "calculating t first calculation results according to the certificate to be signed and the t first sub-secret-keys in the multiple first sub-secret-keys upon receiving a certificate to be signed."

Element 3: "obtaining the second sub-secret-key corresponding to the t first sub-secret-keys according to the equation combination representation; calculating a second calculation result according to the second sub-secret-key obtained and the certificate to be signed."

Brickell at best discloses a cryptographic system in which a password is split into a plurality of password pieces. The password pieces are stored at different remote servers. The different remote servers work together to determine that the user has knowledge of the correct password. If any subnet of the remote server is compromised, the compromised subnet cannot conceive any remaining server that they know the password (see abstract in Brickell). Each of the remote servers receives the password pieces, decrypts the password pieces and compares the decrypted pieces to the pre-registered password pieces for the user, and if the received password pieces match the pre-registered password pieces, the remote server signs an "authentication accept" message (see column 5, line 11-line 17 of Brickell). In Brickell the decrypted password pieces are compared to the pre-registered password pieces to implement the authentication, and the password pieces are not classified into two types, and there is

no corresponding relationship between the password pieces. Therefore, Brickell fails to teach or suggest the above-mentioned Elements 1, 2, and 3 of claim 19 and 1, 2, and 3 of claim 37.

Brennan at best discloses a secure computer system. In the secure computer system, the master key information is separated into a plurality of master key shares which are distributed to master key agents such that each master agent possesses one master key share. The locking key information is separated into a plurality of locking key shares which are distributed to locking key agents such that each locking key agent possesses one locking key share. Then the plurality of locking key shares and the plurality of master key shares are validated, and the secure computer system is securely shut down (see abstract in Brennan). Brennan fails to teach or suggest the above-mentioned Elements 1, 2, and 3 of claim 19 and 1, 2, and 3 of claim 37.

In Frankel the agent has its individual key shares, and calculates a partial result based on its own individual key shares. The individual key shares in the agents are not classified into two kinds of key shares, and there is no corresponding relationship between the individual key shares. The output processor combines the partial results generated by the agents to obtain the result of the cryptographic system according to an equation which is used for calculating the partial results. The equation for combining the partial results is different from the equation combination representations in the amended claim 19, in the caim 19 one second sub-secret-key correspond to the t first sub-secret-keys according to an equation combination representation. The output processor in Frankel is used for combining the partial result, but the matched online

secret combiner in the amended claim 19 is used for not only calculating a second calculation result according to the certificate to be signed and the second sub-secret-key corresponding to the matched equation combination representation, but also calculating a digital signature according to the t first calculation results corresponding to the t items of i and j in the matched equation combination representation and the second calculation result.

Thus it can be easily seen that the amended claim 19 and Frankel are quite different from each other. Brickell and Brennan do not relate to a cryptographic system. Brickell discloses how to split a password and compare the decrypted pieces to the pre-registered password pieces for the user, and the password pieces are not classified into two types, and there is no corresponding relationship between the password pieces. The compromised subnet cannot conceive any remaining server that they know the password when any subnet of the remote server is compromised in Brickell. Brennan discloses a secure computer system which is securely shut down when the plurality of locking key shares and the plurality of master key shares are validated. In Brennan, there is no corresponding relationship between the locking key shares and the master key shares. Therefore, Elements 1 to 3 of claim 19 are not taught nor suggested by any of Brickell and Brennan, or any combination of Frankel, Brickell, and Brennan.

The amended claim 37 is a method claim corresponding to the amended claim 19. Frankel fails to disclose the Elements 1-3 of claim 37. In Frankel, the equation combination representation is not mentioned in the cryptographic system, and the equation in Frankel is used to combine the partial result to a result of the cryptographic

system. The individual key shares in the agents are not divided into two kinds of key shares, and there is no corresponding relationship between the individual key shares. The t first calculation results and the second calculation result are not mentioned in Frankel. Brickell and/or Brennan can not be combined with Frankel to obtain the Elements 1 to 3 of claim 37.

Frankel, Brickell, or Brennan fail to teach or suggest the Elements 1-3 of claim 19 or Elements 1-3 of claim 37, so the amended independent claims 19 and 37 define over the art cited by the Examiner. Likewise, claims 20 to 36, which depend from claim 19, and claims 38 to 40, which depend from claim 37, also define over the prior art.

CONCLUSION

In view of the above amendment, applicant believes the pending application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (248) 641-1600.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 08-0750, under Order No. 9896-000013/US from which the undersigned is authorized to draw.

Dated: August 1, 2007

Respectfully submitted,

By /Joseph M. Lafata/
Joseph M. Lafata
Registration No.: 37,166
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1223
Attorney for Applicant

Attachments